

**Security Schnittstelle
für das
Gesundheitswesen**

Stand der Spezifikation:	Oktober 2008
Version:	1.5.1 Praxiseinsatz ab 01.10.2008
Herausgeber:	Spitzenverbände der gesetzlichen Krankenversicherung
Redaktion - Federführung:	AOK Bundesverband Rosenthaler Straße 31, 10178 Berlin Telefon 030-34646-0 E-Mail: Wolfgang.Strobel@bv.aok.de in Zusammenarbeit mit Informationstechnische Servicestelle der Gesetzlichen Krankenversicherungen GmbH 63094 Rodgau, Postfach 50 01 52 Telefon 06106/85260 - Telefax 06106/852630 E-Mail: info@itsg.de

1	ÄNDERUNGSINFORMATIONEN	4
2	DEFINITION DER SECURITY SCHNITTSTELLE FÜR DAS GESUNDHEITSWESEN	4
2.1	Einleitung	4
2.2	Grundlagen	7
2.3	Vorbemerkungen	8
3	FESTLEGUNGEN	9
3.1	Datenformate	9
3.1.1	Spezifikation: Session-Key	9
3.1.2	Spezifikation: Interchange Key	9
3.1.3	Spezifikation: Hashfunktion/Signaturalgorithmus	9
3.1.4	Spezifikation: RSA Schlüssellänge	9
3.1.5	Spezifikation: Öffentlicher Exponent des RSA Algorithmus	9
3.1.6	Spezifikation: Public-Key Format	10
3.1.7	Spezifikation: Zertifikate	10
3.1.8	PKCS#7 (Public Key Cryptography Standards)	10
3.2	Namenskonventionen	10
3.3	Kommunikation zum Datenaustausch mit der gesetzlichen Krankenversicherung	11
3.4	Gültigkeitszeitraum der Zertifikate	12
3.5	Sperrlisten	13
4	SCHLÜSSELMANAGEMENT	14
4.1	Allgemein	14
4.2	Definition der Zertifikate	15
4.2.1	Versionsnummer	15
4.2.2	Seriennummer	15
4.2.3	Signatur (nur Identifizierung der Algorithmen)	15
4.2.4	Name des Zertifikatserzeugers	15
4.2.5	Gültigkeitsdauer	15
4.2.6	Name des Subjekts	15
4.2.7	Öffentlicher Schlüssel des Teilnehmers	16
4.2.8	Syntax für x.509v3 Zertifikate	16
4.3	Zuordnung der Schlüssel	16
4.4	Gültigkeitsmodell	17
4.5	Management von Sperrlisten	18

5	VERFAHRENSBESCHREIBUNG	19
5.1	Struktur der Zertifizierungshierarchie	19
5.2	Rollen und ihre Funktionen	20
5.3	PCA -Wurzel der Zertifizierungshierarchie	21
5.3.1	Identität der PCA	21
5.3.2	Zuständigkeitsbereich der PCA	21
5.4	Trust Center (Certification Authority)	23
5.4.1	Zertifizierungsanforderung	23
5.4.2	Zertifikatsüberprüfung	24
5.4.3	Eindeutigkeit von Namen	24
5.4.4	Propagierung Zertifizierungsinformation	24
5.4.5	Sperrlisten Management	24
5.4.6	Schlüsselverteilung via Datenträger	25
5.5	Registrierungsstelle (RA = Registration Authority)	27
5.6	Teilnehmer	28
5.7	Erzeugung und Schutz der Teilnehmerschlüssel	28
5.8	Certification Request	29
5.9	Verarbeitung von Sperrlisten	30
6	ANHANG	31
6.1	ASN.1 Syntax relevanter Datenstrukturen	32
6.1.1	Öffentlicher und privater Schlüssel nach X.509	32
6.1.2	X.509v3-Zertifikat, Zertifizierungspfad	33
6.1.3	Sperrliste	34
6.2	ASN.1 Syntax relevanter Makros	35
6.2.1	Signierte Struktur	35
6.2.2	ASN.1 Syntax einer Signatur	36
6.3	Kommunikationssystem	37
6.3.1	Grundsatz	37
6.3.2	Voraussetzungen und Forderungen für den Datenaustausch auf Basis von S/MIME (E-Mail Kommunikation)	37
6.3.3	Voraussetzungen und Forderungen für den Datenaustausch verschlüsselter und ggf. signierter Datenobjekte (Datenträger und sonstige Datenfernübertragungsverfahren)	37

1 Änderungsinformationen

Historie

Aktuelle Version	Oktober 2008	Version 1.5.1
Vorgängerversion	Oktober 2005	Version 1.5
Vorgängerversion	Mai 2003	Version 1.5

Diese Darstellung beschreibt die Änderungen zur jeweiligen Vorgängerversion und soll eine kurze Information über die geänderten Teile des Dokumentes geben.

Seite	Art (neu,geändert, gelöscht)	Kurzbeschreibung der Änderungen zur Vorgängerversion
15	geändert	Ergänzung der Seriennummer um die Verwendung des jeweils jüngsten Zetifikats

2 Definition der Security Schnittstelle für das Gesundheitswesen

2.1 Einleitung

Die folgende Definition einer Security Schnittstelle ist als festgeschriebene, jedoch offengelegte Schnittstelle für das Gesundheitswesen ausgelegt.

Ziel dieser Definitionen ist es, im Gesundheitswesen eine gesicherte digitale Kommunikation unabhängig von der Art der jeweiligen Systeme zu gewährleisten.

Die rasche technische Weiterentwicklung, die Integration der Internet Online-Dienste und die Anforderungen des Signaturgesetzes machen eine Aktualisierung der vorhandenen Definitionen erforderlich. Die vorliegende Fassung (Version 1.5) der Security-Schnittstelle für das Gesundheitswesen ist eine Fortschreibung der bisherigen Definitionen (Version 1.3, Stand: 23.07.2001), die Grundlage für das bestehende Sicherheitsverfahren sind.

Die Konzeption ist als Migrationsstrategie für die bestehenden Sicherheitsverfahren ausgelegt. Die Migrationsansätze sehen vor, dass die vorhandenen Anwendungen für einen bestimmten Zeitrahmen weiter genutzt werden können. Die Beteiligten sollen den Einsatzzeitpunkt für die modifizierten Applikationen, soweit keine unabdingbare Notwendigkeit gegeben ist, selbst bestimmen können. Dementsprechend soll sowohl die heute bestehende, als auch die sich aus den nachfolgenden Definitionen ergebende Security-Technologie bis zum Zeitablauf der im Umlauf befindlichen Teilnehmer-Schlüssel parallel eingesetzt werden können (PKCS#7-/ neben PEM-Verschlüsselung).

Neben den Minimalanforderungen, die durch einen Hersteller erfüllt werden können, der Kommunikations-Applikationen für das Gesundheitswesen anbieten möchte, sind optionale Definitionen mit Blick auf das Signaturgesetz enthalten.

Das Signaturgesetz unterscheidet in Übereinstimmung mit der EG-Signaturrechtlinie folgende Signaturen:

- Elektronische Signatur (§ 2 Nr. 1 SigG),
- fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG),

- qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG),
- qualifizierte elektronische Signatur mit Anbieter-Akkreditierung (§ 15 Abs. 1 Satz 4 SigG).

Die qualifizierte elektronische Signatur dürfte wohl der EG-Mindeststandard sein. Sie hat folgende Merkmale:

- Der Anbieter erklärt, dass die Anforderungen des Signaturgesetzes erfüllt sind (behauptete Sicherheit ohne Nachweis).
- Die Signatur braucht nur mindestens sechs Jahre überprüfbar zu sein (anschließend darf der Anbieter die Zertifikate aus seinen Verzeichnissen löschen).

Die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung – hier ist die Sicherheit nachgewiesen (durch gesetzlich anerkannte fachkundige Dritte) und dauerhaft überprüfbar (mindestens 30 Jahre).

Sicherlich sind alle genannten Arten der elektronischen Signatur je nach Verwendungszweck einsetzbar. Für einige Verfahren ist aufgrund verfahrensrechtlicher Vorschriften die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung vorgeschrieben (nur diese Art ist der eigenhändigen Unterschrift gleichgestellt). Daher sollte auch zur Vermeidung verschiedener Sicherheitsstufen, eine einheitliche Stufe definiert und umgesetzt werden. Es erscheint sinnvoller umfassende Sicherheit zu haben auch für die Kommunikationsabläufe, die dies nicht unbedingt notwendig machen. Daher wird in diesem Papier, soweit eine elektronische Signatur angesprochen wird, von der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung (§ 15 Abs. 1 Satz 4 SigG) ausgegangen.

Angesichts der absehbaren Entwicklungen Signaturgesetzkonformer Verfahren hat sich die Technische Arbeitsgruppe der gesetzlichen Krankenversicherung dafür ausgesprochen, die Weiterentwicklung (im Sinne einer Migration) in verschiedenen Phasen zu realisieren.

In der ersten Phase soll die Umstellung auf PKCS#7-basierende Verschlüsselungsverfahren erfolgen. Neben den daraus resultierenden zwangsläufigen Anpassungen soll in dieser Phase die Aktualisierung der Schlüssellänge des RSA-Algorithmus realisiert werden. Weiterhin wird als Hash-Funktion der SHA-1 Algorithmus der Einsatz von X.509 v3-Zertifikaten (ISIS-MTT Spezifikationen V1.0.2) und die Verwendung des Triple-DES mit dieser ersten Phase vorgeschrieben. Die Nutzung von LDAP steht unter dem Vorbehalt einer Kosten-Nutzen-Analyse.

Die in diesem Dokument dargestellten Änderungen gegenüber der Version 1.3 im Zusammenhang mit einer Umstellung von PEM nach MIME bzw. S/MIME sollen Gegenstand einer späteren Umstellungsphase sein. Bis dahin gelten insoweit die Spezifikationen der Version 1.3 (PEM) unverändert weiter. Dies betrifft im besonderen die Ausführungen zu den Datenformaten (2.1), zur Zertifizierungsanforderung (4.4.1), zum Certification Request (4.8) und zum Kommunikationssystem (5.3).

Mit dieser Vorgehensweise sollen die „weitreichenden“ Verfahrensänderungen, die Zusammenhang mit einer Umstellung von der File-Verschlüsselung (PEM) zur E-Mail-Verschlüsselung (S/MIME) entstehen, vermieden werden.

Aufgrund des bereits erwähnten hohen Bedürfnisses nach einer Sicherung der elektronischen Prozesse, verläuft die technologische Weiterentwicklung von PKI-Produkten rasant. Die in diesem Papier beschriebenen notwendigen Modifikationen sollen im Sinne einer Migrations- Strategie in einem Phasenmodell erfolgen. Damit soll u. a. erreicht werden, dass die laufenden Prozesse nicht beeinträchtigt werden.

Bis zum Ablauf der Gültigkeit der vorhandenen Zertifikate wird die Koexistenz und soweit erforderlich, die Interoperabilität der vorhandenen und der „neuen“ Systemes vorausgesetzt.

Die Migrationsschritte analog des Phasenmodells stellen sich im einzelnen wie folgt dar:

Phase 1

1. ab Herbst 2003 wird ein Test der Basiskomponenten mit ausgewählten Kommunikationspartnern durchgeführt. Die Beteiligung erfolgt auf freiwilliger Grundlage, soweit die Voraussetzungen im Einzelfall gegeben sind. Die ITSG-GmbH stellt den Testteilnehmern der GKV-Verbände (bzw. deren Datenannahmestellen) bei entsprechender Bedarfsmeldung (z. B. wenn die jeweilige interne Applikation den Anforderungen bis dahin nicht genügt), eine PKCS#7-basierende Komponente (ohne Support) zur Verfügung.
2. Ab 01.12.2003 beteiligt sich mindestens eine Datenannahmestelle jeder Kasenart am Testverfahren.
3. Ab 01.07.2004 nehmen Datenannahmestellen am beschriebenen Testverfahren teil. Angestrebtes Ziel ist es dabei, die Tests auf der Grundlage der jeweiligen, den beschriebenen Anforderungen angepassten internen Applikationen, durchzuführen.
4. Die Entwicklungen und Erprobungen sind bis 31.12.2004 abgeschlossen. Der Praxisbetrieb im Parallelverfahren (Ausgangs- und Zielsystem) beginnt frühestens am 01.01.2005.

Die Koordination der vorbeschriebenen Phase 1 wird für alle Testteilnehmer von der ITSG GmbH wahrgenommen.

Die dargestellte Zeitrahmen ist als erste Planung zu verstehen. Soweit sich im weiteren Verlauf Erkenntnisse oder Notwendigkeiten ergeben, die dahingehende Änderungen erforderlich machen, werden in gemeinsamer Abstimmung zwischen den Beteiligten die entsprechenden Korrekturen vorgenommen.

2.2 Grundlagen

Generelle Forderungen an die Sicherheitsdienste sind die Vertraulichkeit, die Integrität, die Authentifikation sowie die Verbindlichkeit der Kommunikation.

Als grundlegendes Verfahren der Sicherheitstechnologie nimmt die kryptographische Technik die zentrale Rolle auch in der angestrebten PKI ein. Die Verfahren sollen folgenden Ansprüchen genügen, bzw. die ersten Voraussetzungen dafür schaffen:

- RSA-Algorithmus mit 2048 Bit Schlüssellänge
- Triple-DES-Algorithmus (X9.17)
- SHA-1 Algorithmus (160 Bit) oder RIPEMD-160
- X.509 v3-Zertifikate (ISIS-MTT Spezifikationen V1.0.2)
- lokale und zentrale Generierung von Schlüsseln
- Schnittstellen zu Sicherheitstoken (Chipkarten)
- PKCS#7 – elektronische Signatur und Verschlüsselung
- S/MIME-Nachrichten (Version 3)
Nachrichtenaustauschformate nach ISIS-MTT (V1.0.2), für signierte Nachrichten: Nachrichtentyp „opaque“
- Verzeichnisdienst
- Transportprotokoll (LDAP v3)
- Bei Verwendung von Chipkarten ist die MailTrust-Spezifikation der Token-Schnittstelle (nach ISIS-MTT/MTT-Cryptoki-Spezifikation), die auf dem „Cryptographic Token Interface Standard [PKCS11 97] beruht, vorzusehen.

Die vorgesehenen 2048 bzw. 160-Bit basierenden Verschlüsselungsfunktionen bieten nach heutigem Kenntnisstand eine langfristige Sicherheit. Die bekannten Analysen in diesem Zusammenhang ergeben, dass damit von einer Sicherheit der Kryptoalgorithmen für mindestens die nächsten 6 Jahre ausgegangen werden kann.

Aufgrund der Schlüssellängen ist mit erheblichen Laufzeitveränderungen zu rechnen. Soweit dahingehende Erfordernisse auftreten, können die Schlüssellängen nach gemeinsamer Abstimmung entsprechend verändert werden.

2.3 Vorbemerkungen

Es werden derzeit auf dem Markt verschiedene Verfahren für die Generierung von Sicherheitsfunktionen angeboten. Die bedeutenden Verfahren haben im allgemeinen gleiche Konstruktionsmerkmale, unterscheiden sich in Details.

Grundlage sind die MailTrust (ISIS-MTT V1.0.2) Spezifikationen für das PKI-Management, welche sich im wesentlichen an den Spezifikationen des PKIX-Dokumentes „Certificate Management Protocols [PKIX-CMP 98] orientieren. Da kein „neues“ Verfahren dem Sinne nach konzipiert wird, wurde auf vorhandene Funktionalitäten aufgebaut und das Fachwissen am Markt etablierter Hersteller/Anbieter von Security-Software und TeleTrust Deutschland e. V. integriert.

Grundlage des Schlüsselmanagements ist die Verwendung von Zertifikaten, um öffentliche Schlüsselinformationen authentisch dem Sender und dem Empfänger einer Nachricht zur Verfügung zu stellen.

Derzeitige Basis des Ansatzes bilden dabei die in den RFC1421 - RFC1424 festgelegten Grundlagen zu Electronic Mail unter Verwendung von PEM-Mechanismen).

In der nächsten Phase der Weiterentwicklung orientiert sich das Management von Zertifikaten und Schlüsseln an Standards (Basis des Ansatzes bildet z. B. CMC – Certificate Management Messages over CMS) – siehe auch RFC 2797. Diese Festlegung ist mit Hinblick auf die Trust Center Betreiber sinnvoll. Damit ist die Beantragung von Zertifikaten über PKCS#10 und PKCS#7 neben CMP vorgesehen. Der ausschließliche Verweis auf CMP unterstellt, dass eine Vielzahl an Nachrichtentypen zu unterstützen wären, die aber zum Teil für das Verfahren nicht bedeutend sind.

Die Zertifikatsformate X.509v3 werden entsprechend in der ASN.1-Syntax beschrieben. Erklärtes Ziel ist es, eine Absprache bezüglich einiger Parameter zu treffen, um für das Sicherheitsverfahren im Gesundheitswesen eine, auch im Hinblick auf die Zukunft, sichere Kommunikation zu gewährleisten. Dieses Ziel kann nur durch die Beteiligung der am Markt etablierten Anbieter und Hersteller von Sicherheitssoftware, die i.d.R. dem TeleTrust Deutschland e. V. angehören, erreicht werden. Die vorliegende Dokumentation folgt einem international konsolidierten Konzept für Informations- und Kommunikationssicherheit in offenen IT-Systemen. Die Auswahl der Algorithmen und Schlüsseldefinitionen, der Datenformate, der Zertifizierungsstruktur und der Struktur der Adressen für die Schnittstelle sind Grundlage dafür, dass

- die Interoperabilität von Anwendungen,
- die Interoperabilität zwischen Zertifizierungsinstanzen beim Schlüsselmanagement und anderen Trusted Third Party - Diensten,
- die Bereitstellung von miteinander kompatiblen Hard- und Softwarekomponenten und Diensten durch Technologie- und Produktentwickler

gewährleistet werden können.

Dieses Dokument ist nicht abschließend, sondern soll und wird im Verlaufe der weiteren Aktivitäten, insbesondere nach den Anforderungen und Erkenntnissen im Verlauf der Weiterentwicklung entsprechend aktualisiert.

Die aufgeführten Spezifikationen orientieren sich an etablierten Standards (z.B. X.509 und PKCS#11). Die im Einsatz befindlichen Verfahren sind im Rahmen der Migration entsprechend zu berücksichtigen.

Die Spezifikationen beschreiben die Minimalanforderungen, die zur Teilnahme am Verfahren zu erfüllen sind.

3 Festlegungen

Die Sicherheitsstruktur beschreibt die Komponenten und Prozeduren der erforderlichen Sicherheitsinfrastruktur, der Zertifizierungsstrukturen und des Schlüsselmanagements.

3.1 Datenformate

Die S/MIME-Nachrichten (als Kombination von MIME-Bodies und geschützten weiteren Inhalten) sind entsprechend S/MIME (Version 3) [RFC 2633 u. 2632] zu strukturieren (Schnittstelle zur Kommunikation der Applikationen - PKCS#11).

Um den Verfahrensablauf nicht zu gefährden, reicht es aus, die Funktionen zu unterstützen, die bereits in S/MIME Version 2 [RFC 2312 und 2311] spezifiziert sind.

Datenaustauschformate und Nachrichtentypen gemäß der ISIS-MTT V1.0.2 Spezifikation.

Für signierte Nachrichten: "Opaque Signed" (im Sinne von „Clear Signed Date“ Empfänger ohne S/MIME können den Nachrichteninhalt zwar lesen, die Signatur jedoch nicht überprüfen – Format „Multipart Signed“);

für verschlüsselte Nachrichten: „Enveloped Data“.

3.1.1 Spezifikation: Session-Key

Als Session-Key ist tripleDES (des-ede3-cbc) vorzusehen.

3.1.2 Spezifikation: Interchange Key

Als Interchange Key ist RSA mit den unten beschriebenen Parametern einzusetzen.

3.1.3 Spezifikation: Hashfunktion/Signaturalgorithmus

Als Hash Funktion ist SHA-1 vorzusehen.

Erzeugen eines Message Digest, mit dem die elektronische Unterschrift gebildet wird.

3.1.4 Spezifikation: RSA Schlüssellänge

Die RSA Schlüssellänge beträgt:

PCA-Schlüssel	2048 bit (Standard); nach gesonderter Festlegung auch größer
CA-Schlüssel	2048 bit (Standard); nach gesonderter Festlegung auch größer
Teilnehmer	2048 bit (Standard); nach gesonderter Festlegung 1024 bit

3.1.5 Spezifikation: Öffentlicher Exponent des RSA Algorithmus

Als RSA Exponent soll die Fermat-4 Zahl ($2^{16} + 1$) gewählt werden (siehe X.509).

3.1.6 Spezifikation: Public-Key Format

Hier ist die ASN.1 Syntax Notation sowie X.509 einzuhalten.

3.1.7 Spezifikation: Zertifikate

X.509 V3-Zertifikate (Extensions soweit deren Unterstützung gefordert). Die Komponenten sind so einzustellen, dass OIDs für Extensions in Zertifikaten, die nicht bekannt sind, ignoriert werden. Damit ist eine Verfahrenserweiterung und die Nutzung spezifischer Extensions möglich.

Zertifikate sind in ASN.1 Syntax Notation sowie entsprechend X.509 zu implementieren. Bei der Codierung der Zertifikate sind die Distinguished Encoding Rules (DER) entsprechend X.509, Kapitel 8.7 einzuhalten.

Die Extensions „AuthorityKey-Identifizier; KeyUsage;CertificatesPolicies; SubjectAlternative-Name; BasicConstraints; CRLDistributions_Points“ müssen unterstützt werden.

Die Erweiterung BasicConstraints dient der Erkennung von CA-Zertifikaten. Die Erweiterung umfasst die Felder CA und PathLenConstraint. Das CA-Feld von BasicConstraints enthält den Wert TRUE (Teilnehmer darf Zertifikate signieren). Das Feld PathLenConstraint kann gesetzt sein. Wenn gegeben, ist die Pfadlänge auf 0 zu setzen, soweit die Zertifizierungsstelle ausschließlich Teilnehmerzertifikate (keine Zertifikate für andere CAs) ausstellen darf.

3.1.8 PKCS#7 (Public Key Cryptography Standards)

Beschreibt die allgemeine Syntax für Dateien, die mit kryptografischen Methoden/Funktionen (Verschlüsselung und elektronisch Signatur) bearbeitet werden können. S/MIME-Nachrichten verwenden die in PKCS #7 definierten Standards für die Verwendung von kryptographischen Verfahren mit Hilfe des MIME-Typus application/pkcs7-mime.

3.2 Namenskonventionen

Die unter X.500 vorzuhaltende Namenskonvention lautet:

C	=	Country	(DE)
O	=	Organization	(Name des Trust Centers)
OU	=	Organization Unit	(Name der Institution)
OU	=	Organization Unit	(IK-Nummer oder Betriebsnummer der Institution)
CN	=	Common Name (Allgemeiner Name)	(Name des Ansprechpartner)

Die für die OU-Segmente gewählten Konventionen können im Rahmen der Pilotverfahren und der Interoperabilitätstests angepasst und sowie um weitere OU-Segmente ergänzt werden.

Für die Zertifizierungsstellen lautet die unter X.500 vorzuhaltende Namenskonvention:

C	=	Country	(DE)
O	=	Organization	(Name des Trust Centers)

Als Zeichensatz zur einheitlichen Darstellungsform ist US-ASCII vorzusehen (Zeilenende CR/LF).

3.3 Kommunikation zum Datenaustausch mit der gesetzlichen Krankenversicherung

Sowohl die Trust Center als auch die zur Verfügung stehenden Sicherheitssysteme decken derzeit die Anforderungen einer X.500 Implementierung nicht ab. Die Anzahl an Zertifikaten und auch die mittelfristig erwarteten Teilnehmerzahlen ermöglichen den kompletten Austausch der Verzeichnisse auf der Grundlage der heute verwendeten TCP/IP-Protokollfamilie mittels Email, ftp oder http. Die Basis hierfür bildet die heutige Ausrichtung des Datenaustauschverfahrens innerhalb der GKV.

Für den Aufruf von Zertifikaten und Sperrlisten wird ein Protokoll benötigt, welches Funktionalitäten bietet, wie z. B. das selektive Suchen in Verzeichnissen usw.. Hier bietet LDAP (Lighthouse Directory Access Protocol) v2 [RFC 1778 95] die geeigneten Funktionalitäten für den Verzeichnisabruf. Das Verzeichnis muß dem X.500 Modell entsprechen. Zertifikate und Sperrlisten müssen als Werte vom Typ undefined codiert und in ihrer BER-codierten Form als Binärwerte dargestellt werden. Bei der Nutzung von LDAP sind in Anlehnung an die MailTrust (ISIS-MTT V1.0.2) Spezifikationen mindestens die Operationen: „bind; search und unbind“ vorzusehen. Die Attribute werden binär kodiert. Es soll zeitnah unter Beachtung der wachsenden Teilnehmerzahl und wirtschaftlicher Aspekte die Unterstützung des genannten Verzeichnisdienstes zwischen den Beteiligten abgestimmt werden. Dabei sind in Anlehnung an die aktuell gültigen MailTrust Spezifikationen die diesbezüglichen Vorgaben zu den Austauschformaten zu berücksichtigen.

Als Datei-Extensions sind anzugeben :

Revocation List:	crl
S/MIME (Zertifizierungsantwort)	.p7c
S/MIME (Zertifizierungsanfrage)	.p10

3.4 Gültigkeitszeitraum der Zertifikate

Die Teilnehmer-Zertifikate haben gemäß der Festlegung der Spitzenverbände der GKV die einheitliche Gültigkeitsdauer von drei Jahren.

Es kann nicht ausgeschlossen werden, dass einzelne Trust Center bzw. die einzelne CA (Certification Authority) im Rahmen ihrer Dienstleistung einen davon abweichenden, kürzeren Zeitraum für die Gültigkeit ihrer Zertifikate vorsehen.

Für die PCA (Policy Certification Authority) beträgt die Gültigkeitsdauer des Zertifikates 7 Jahre und für die CA 5 Jahre.

Die Security Schnittstelle sieht die Anwendung eines Schalenmodells für die Zertifikathierarchie vor. Voraussetzung für Anwendungen, die das Schalenmodell unterstützen ist dabei, dass die Laufzeit eines Zertifikats vollständig innerhalb der Laufzeit des ausstellenden (CA-) Zertifikates liegt. Dies wird dann zu einem Problem, wenn die CA-Zertifikate nicht mehr lange gültig sind, da man dann nur noch für den verbleibenden Zeitraum Zertifikate ausstellen kann. Um dieses Problem zu beheben, hat das Zertifikat der PCA eine Laufzeit von 7 Jahren. Bereits nach fünf Jahren wird das nächste Zertifikat erzeugt, mit dem von da an zertifiziert wird (das alte Zertifikat stellt dann nur noch die Gültigkeit der vorher ausgestellten Zertifikate, insbesondere durch die regelmäßige Erzeugung aktueller Sperrlisten, sicher). Somit ist es für die PCA jederzeit möglich, CA-Zertifikate mit einer Laufzeit von 5 Jahren zu erzeugen.

Die beteiligten Trust Center sind verantwortlich für die Einhaltung dieser Konvention. Sie prüfen vor der jeweiligen Teilnehmerzertifizierung die Laufzeiten des eigenen CA-Zertifikats und des PCA-Zertifikats und stellen sicher, dass die Laufzeiten nicht überschritten werden. Dazu beantragen die Trust Center rechtzeitig vor dem Auslauf des CA-Zertifikates die Neu-Zertifizierung durch die PCA.

3.5 Sperrlisten

Die Verarbeitung der jeweils aktuellen Sperrlisten wird vorausgesetzt. Die Definition der Profile für Zertifikate und Sperrlisten entspricht den MTTv2-Spezifikationen.

Analog dem vorgesehenen Gültigkeitsmodell ist die Gültigkeit von Schlüssel und Zertifikaten entsprechend MTTv2 als sogenanntes „Schalenmodell“ ausreichend definiert.

Auf dieser Grundlage haben die Teilnehmer auf eigenes Risiko zu bestimmen, ob und in welchen Intervallen Sperrlisten herangezogen werden.

4 Schlüsselmanagement

4.1 Allgemein

Die Integration eines asymmetrischen (Public-Key-Verfahren) Schlüsselmanagements begründet sich auf der Einrichtung einer vertrauenswürdigen Instanz (der Certification Authority - CA), der Schlüsselverwaltungsstelle oder dem Trust Center. Aufgabe des Trust Centers ist es, kryptographische Schlüssel sicher zu erzeugen, zu verwalten und zu verteilen. Das Schlüsselmanagement basiert auf der Verwendung von Zertifikaten zur Propagierung von öffentlicher Schlüssel an Kommunikationspartner.

Das beschriebene Schlüsselmanagement umfasst insbesondere:

- die Zertifizierungshierarchie,
- die Zertifikate,
- die Erzeugung und Prüfung von Zertifikaten,
- das Sperrlistenmanagement sowie
- die Rollen innerhalb der Systemarchitektur.

Die öffentlichen Teilnehmerschlüssel werden durch eine vertrauenswürdige Instanz - der Certification Authority (CA) - zertifiziert. Dazu werden die öffentlichen Teilnehmerschlüssel in Form einer komplexen von der CA signierten Datenstruktur im System propagiert. Die Spezifikation der Zertifikate basiert auf dem aktuellen Zertifikatsformat X.509v3 (ITU-T X.509 97). Gegenüber dem bisherigen Zertifikatsformat sind zusätzliche Felder im Sinne von Zertifikatserweiterungen möglich.

Die Zertifikatsverifizierung durch den Leistungserbringer oder Arbeitgeber wird durch die Überprüfung der zugehörigen Gültigkeitsdauer und dem Abgleich einer durch die CA verteilten Sperrliste abgeschlossen. Die Identitäten von Subjekt und CA sind sogenannte „Distinguished Names“, wie sie in X.500 festgelegt sind.

4.2 Definition der Zertifikate

Die folgende Definition der Zertifikate enthält aufgrund des gewählten Ansatzes einer konzeptionellen Darstellung keine direkten Spezifikationen der Datenfelder. Zertifikate sind die zentralen Datenstrukturen innerhalb des Schlüsselmanagements für X.509 und S/MIME. Dieser Abschnitt enthält einen Überblick über die Inhalte eines Zertifikats. Im Anhang A.3 befindet sich die ASN.1 Syntax eines X.509v3-Zertifikats. Ein Zertifikat besteht danach aus den folgenden Datenfeldern:

4.2.1 Versionsnummer

Anhand der Versionsnummer können unterschiedliche Formate (z. B. nach einer Änderung der Struktur) unterschieden werden. Das V3 Zertifikat wird mit dem Wert „2“ angezeigt.

4.2.2 Seriennummer

Die Seriennummer, ggf. mit führenden Nullen, ist eine eindeutige Nummer bezüglich derjenigen Zertifikate, die von einem Zertifikatserzeuger ausgegeben werden (identifiziert ein Zertifikat entsprechend der CA-Aussteller). Das Paar bestehend aus Name des Zertifikatserzeugers und Seriennummer muss weltweit eindeutig sein. Ein Zertifikatserzeuger muss garantieren, dass je zwei verschiedene Zertifikate mit dem gleichen Namen des Zertifikatserzeugers unterschiedliche Seriennummern besitzen. Die Seriennummer wird zur Identifizierung eines Zertifikates innerhalb von Sperrlisten verwendet. Ein Teilnehmer mit mehr als einem gültigen Zertifikat soll für den Datenaustausch in der GKV stets das Zertifikat mit der höchsten Seriennummer, bzw. bezogen auf die Gültigkeit das jüngste Zertifikat verwenden. Bei Antworten an den Teilnehmer werden von den Datenstellen der Krankenkassen die Nachrichten jeweils mit dem jüngsten Zertifikat des Teilnehmers verschlüsselt.

4.2.3 Signatur (nur Identifizierung der Algorithmen)

Dieses Datenfeld informiert über den Algorithmus und die zugehörigen Parameter, die vom Zertifikatserzeuger zur Signaturbildung verwendet werden.

4.2.4 Name des Zertifikatserzeugers

Dieses Datenfeld enthält die Identität des Zertifikatserzeugers in Form eines "Distinguished Name" nach X.500. Diese Identifikation ist Voraussetzung zur korrekten Auswahl des öffentlichen Schlüssels mit dem (u.a.) das Zertifikat verifiziert wird. Der Zertifikatserzeuger ist eine Certification Authority (PCA oder CA), die die Zusammengehörigkeit der Teilnehmeridentität und des zugehörigen öffentlichen Schlüssels bestätigt.

4.2.5 Gültigkeitsdauer

Beinhaltet die Gültigkeitsdauer eines Zertifikates in Form eines Start- und Endzeitpunkts. Als Zeitformat ist „GeneralizedTime“ zu verwenden (Format: YYMMDDHHMMSSZ).

4.2.6 Name des Subjekts

Dieses Datenfeld enthält die weltweit eindeutige Identität des Systemteilnehmers (Distinguished Name). Mit dem Zertifikat bestätigt der Zertifikatserzeuger die Zuordnung zwischen Teilnehmeridentität und öffentlichem Schlüssel. Die Syntax des Datenfeldes richtet sich nach der X.500-Struktur (Distinguished Names).

4.2.7 Öffentlicher Schlüssel des Teilnehmers

Inhalt dieses Datenfeldes `subjectPublicKeyInfo` ist der öffentliche Schlüssel des Teilnehmers sowie ein Algorithmus-Identifizier.

4.2.8 Syntax für x.509v3 Zertifikate

Der X.509v3 Standard beinhaltet eine Vielzahl an Zertifikatserweiterungen. Die Zertifikate und Sperrlisten müssen die für die Prüfung der Gültigkeit (einschließlich der elektronischen Signatur) notwendigen Informationen enthalten. Soweit daneben Extensions verwendet werden, ist eine vorherige Abstimmung zwischen allen am Verfahren beteiligten erforderlich. Als Basis gelten die Festlegungen der Profile für Zertifikate und Sperrlisten nach den entsprechenden MTTv2 -Spezifikationen.

4.3 Zuordnung der Schlüssel

Die übergeordnete **Policy Certification Authority (PCA)** verwaltet die folgenden Schlüssel:

- Den öffentlichen Schlüssel der Wurzel der Zertifizierungshierarchie.
- Das eigene Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel.

Diese Schlüssel werden zur Zertifikatserzeugung (privater Schlüssel) und -prüfung (öffentlicher Schlüssel) verwendet.

Jede **Certification Authority (CA)** hält die folgenden Schlüssel vor:

- Den öffentlichen Schlüssel der Wurzel der Zertifizierungshierarchie.
- Den aktuellen öffentlichen Schlüssel der übergeordneten PCA in Form eines Zertifikats.
- Das eigene Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel.

Diese Schlüssel werden zur Zertifikatserzeugung (privater Schlüssel) und -prüfung (öffentlicher Schlüssel) verwendet.

Jeder **Teilnehmer (UA – User Agent)** hält die folgenden Schlüssel vor:

- Den öffentlichen Schlüssel der Wurzel der Zertifizierungshierarchie.
- Den aktuellen öffentlichen Schlüssel der übergeordneten PCA in Form eines Zertifikats und der aktuelle öffentliche Schlüssel der CA (Zertifikat der übergeordneten PCA) in Form eines Zertifikats.
- Das eigene Schlüsselpaar bestehend aus dem privaten und zertifizierten öffentlichen Teilnehmerschlüssel.
- Die aktuellen öffentlichen Schlüssel aller anderen Systemteilnehmer (optional: Zugriff auf das X.500-Directory).

Es ist zu beachten, dass u. U. mehr als ein Schlüsselpaar (theoretisch unbegrenzt viele) vorhanden sein kann, also verwaltet werden muss.

4.4 Gültigkeitsmodell

In allen Produkten sind Prozeduren zur Prüfung der Gültigkeit von Schlüsseln und Zertifikaten vorzusehen.

In Anlehnung an das Schalenmodell der MTTv2 Spezifikationen (gelten auch für die Prüfung des Zertifizierungspfades) ergibt sich die Gültigkeit von Zertifikaten und Schlüsseln:

- Ein Schlüssel ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn zu diesem Zeitpunkt der zugehörige Zertifizierungspfad gültig ist.
- Ein Zertifizierungspfad ist zu einem bestimmten Zeitpunkt genau dann gültig, wenn alle in ihm enthaltenen Zertifikate zu diesem Zeitpunkt gültig sind.

Ein Zertifikat ist zu einem Zeitpunkt genau dann gültig, wenn

- Die Signatur korrekt ist (Vergleich von Hashwerten).
- Der fragliche Zeitpunkt innerhalb des Gültigkeitszeitraumes des Zertifikats liegt.
- Alle als kritisch markierten Extensions des Zertifikats die dafür definierten Prüfungen erfolgreich durchlaufen haben.
- Das Zertifikat nicht in einer der zum fraglichen Zeitpunkt aktuellen Sperrlisten für das Zertifikat enthalten ist, die vom Verifizierer gewünschten Sperrinformationen enthalten, das Zertifikat zwar in einer solchen Sperrliste enthalten ist, der angegebene Sperrzeitpunkt jedoch nach dem fraglichen Zeitpunkt liegt, oder die Sperrliste ein Testattribut enthält.

4.5 Management von Sperrlisten

Die Sperrlisten werden in regelmäßigen Abständen (bei jeder Änderung) innerhalb des Verzeichnisdienstes veröffentlicht. Unter Bezug auf das Gültigkeitsmodell ist der aktuelle Abruf der Sperrlisten notwendig (Empfehlung - tagesaktueller Abruf).

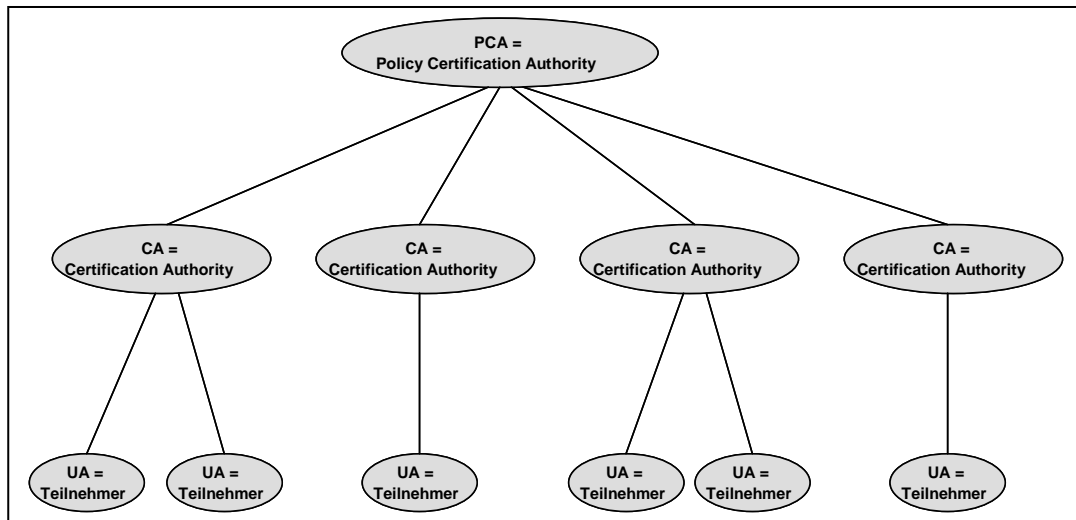
Analog dem vorgesehenen Gültigkeitsmodell ist die Gültigkeit von Schlüssel und Zertifikaten entsprechend MTTv2 als sogenanntes „Schalenmodell“ ausreichend definiert.

Auf dieser Grundlage haben die Teilnehmer auf eigenes Risiko zu bestimmen, ob und in welchen Intervallen Sperrlisten herangezogen werden.

5 Verfahrensbeschreibung

5.1 Struktur der Zertifizierungshierarchie

Die Zertifizierungshierarchie folgt nachfolgendem Aufbau.



Die oberste Wurzel des Zertifizierungsbaumes ist die Policy Certification Authority. Auf der nächsten Ebene der Zertifizierungshierarchie befinden sich die CA'en um Teilnehmer und weitere Strukturen einer Organisation zu zertifizieren. Zur Zeit wird die PCA gebildet durch die Kooperationsgemeinschaft Trust Center unter Leitung der Informationstechnischen Servicestelle der gesetzlichen Krankenversicherung (ITSG GmbH). Dieser Arbeitsgemeinschaft PCA gehören derzeit die DKTIG GmbH, die BfA und der VDR an. Der Vertrag zur Kooperation regelt den Zutritt weiterer Trust Center, sofern die Bedingungen der Policy der PCA erfüllt werden.

5.2 Rollen und ihre Funktionen

Die Systemarchitektur wird anhand der im System vorhandenen Rollen und ihren Funktionalitäten beschrieben. Innerhalb der Architektur können danach die folgenden vier Rollen identifiziert werden:

- Teilnehmer (UA),
- Zertifizierungstelle (CA),
- Registrierungsstelle (RA) und
- Verzeichnisdienst (DIR).

5.3 PCA -Wurzel der Zertifizierungshierarchie

Die PCA (Policy Certification Authority) verfügt über eine Policy, in dem die PCA-Sicherheitspolitik festgelegt wird. Eine signierte Kopie dieses Dokumentes wird allgemein verfügbar gemacht. Die Autorisierung einer CA, innerhalb der Zertifizierungshierarchie zu operieren, basiert auf diesem Dokument sowie auf dem herausgegebenen Zertifikat der PCA.

Die Sicherheitspolitik folgt dabei den Sicherheitsleitlinien einer obersten Zertifizierungsstelle, die allgemein als Policy Certification Authority (PCA) bezeichnet wird. In Ermangelung einer anderen geeigneten und verfügbaren Instanz haben sich die von den

Spitzenverbänden der gesetzlichen Krankenkassen eingerichtete
**Informationstechnische Servicestelle der
Gesetzlichen Krankenversicherung GmbH (ITSG)**

die von der Deutsche Krankenhausgesellschaft eingerichtete
**Deutsche Krankenhaus TrustCenter und
Informationsverarbeitung GmbH (DKTIG)**

der
Verband Deutscher Rentenversicherungsträger (VDR)

und die
Bundesversicherungsanstalt für Angestellte (BfA),

auf die gemeinsame Gestaltung der PCA Datenermittlung im Gesundheits- und Sozialwesen und deren Policy verständigt.

5.3.1 Identität der PCA

Die o.g. Organisationen betreiben die PCA als gleichberechtigte Partner. Mit dem Aufbau und der Wahrnehmung der DV-technischen Aufgaben der PCA ist derzeit die Competence Center Informatik (CCI) GmbH betraut.

5.3.2 Zuständigkeitsbereich der PCA

Als Zuständigkeitsbereich der PCA ist vorrangig das deutsche Gesundheits- und Sozialwesen vorgesehen. Das primäre Ziel besteht in der Sicherung der Kommunikation im Rahmen des Datenaustausches zwischen der GKV, GRV und allen Leistungserbringern, die über eine IK-Nummer, sowie Arbeitgebern, die über eine Betriebsnummer verfügen.

Der Name der PCA wurde daher so gewählt, dass nicht nur CA's aus dem Gesundheitswesen oder dem Bereich der Rentenversicherung, sondern darüber hinaus ggf. auch CA's und Teilnehmer aus anderen Bereichen des Sozialwesens im Interesse einer für alle Beteiligten vereinfachten Gestaltung der CA (insbesondere auch im Hinblick auf den Austausch der von ihnen zertifizierten Schlüssel) die Funktion der PCA in Anspruch nehmen können.

PCAs sollten substantiell unterschiedliche Sicherheitsleitlinien haben. Für das deutsche Gesundheits- und Sozialwesen sind aus Sicht der genannten Partner substantiell unterschiedliche Sicherheitsleitlinien nicht erforderlich. Darüber hinaus sind die vorhandenen Sicherheitsleitlinien auch für weitere Bereiche des Sozialwesens ausreichend (z.B. für Arbeitgeber für die Übermittlung von DEÜV-Meldungen und Beitragsnachweise).

5.4 Trust Center (Certification Authority)

5.4.1 Zertifizierungsanforderung

Die CA (Trust Center) generiert auf Anfrage ein Zertifikat das u.a. den Namen des Systemteilnehmers, den öffentlichen Schlüssel sowie den Namen des Zertifikatserzeugers enthält. Dabei signiert die CA diese Daten unter Verwendung ihres privaten Schlüssels. Für diesen Vorgang sind vom Teilnehmer bzw. UA mindestens der öffentliche Schlüssel und der Name mitzuteilen. Innerhalb dieses Prozesses ist es erforderlich, dass die CA den Teilnehmer authentisiert, d. h. sich von der Korrektheit der Teilnehmeridentität überzeugt, bevor sie die Zusammengehörigkeit von Teilnehmername und öffentlichem Schlüssel durch das zu erzeugende Zertifikat bestätigt (siehe RA). Die dazu eingesetzten Mechanismen werden durch die CA festgelegt.

Optional:

Alternativ dazu kann auf Anforderung die Schlüsselerzeugung auch durch die CA vorgenommen werden. Der private Schlüssel ist dann auf vertrauliche Weise an den Teilnehmer zu übermitteln.

Zur Certification Request (Zertifikatsanforderung) durch einen Teilnehmer an eine CA werden im folgenden die zwei Varianten

- Anforderung mittels in MIME eingebettetes PKCS#10-Objekt per E-Mail
- Schlüsselverteilung via Datenträger (z. B. Chipkarte)

beschrieben. Im ersten Fall erfolgt die Kommunikation zwischen dem Teilnehmer und dem Trust Center mittels E-Mail. Optional können Trust Center weitere Kommunikationswege unterstützen.

Sie unterscheiden sich durch die von der CA vorgenommenen Form der Authentikation der anfordernden Teilnehmer.

Optional:

Eine Schlüsselverteilung über Datenträger (z.B. Chipkarte) kann gewählt werden, sofern für die Schlüssel zentral von den CA's (Trust Center) vergeben werden. In diesem Fall erzeugt die CA die vollständige Schlüsselinformation (privater Schlüssel und Zertifikat) und übergibt diese dem anfordernden Teilnehmer.

5.4.2 Zertifikatsüberprüfung

Ein erster Schritt einer jeden Zertifikatsprüfung ist die Verifizierung der Signatur des Zertifikatserzeugers unter Verwendung des zugehörigen öffentlichen Schlüssels.

Die Prüfung umfasst folgende Schritte:

1. Erfolgreiche Validierung des Certification Requests (PKCS#10),
2. erfolgreiche Verifizierung der Signatur bzw. des Hashwertes des öffentlichen Schlüssels,
3. sowie einer positiven Konsistenzprüfung beider Nachrichteninhalte.
4. Der Teilnehmer bzw. Antragsteller erhält eine entsprechende Nachricht, sofern die Prüfung ein negatives Ergebnis erbringt.

5.4.3 Eindeutigkeit von Namen

Eine wesentliche Anforderung an das Zertifizierungsschema ist die Eigenschaft der Namens-eindeutigkeit aller Knoten und insbesondere aller zertifizierenden Trust Center.

Bei Zertifizierung einer CA richtet die zertifizierende PCA / CA eine Anfrage an die Datenbank. Besteht kein Konflikt bezüglich dieses Datums, so kann die CA in der Datenbank registriert werden. Dazu sind von der PCA / CA Name, öffentlicher Schlüssel und Name der CA anzugeben.

5.4.4 Propagierung Zertifizierungsinformation

Jeder Sender einer signierten Nachricht muss dem Empfänger die notwendige Zertifizierungsinformation zur Verfügung stellen, d. h. im Zweifelsfalle die vollständige Information, um alle Zertifikate des Zertifizierungspfads verifizieren zu können.

Steht ein geeignetes Public Directory zur Verfügung, so kann auf die Übermittlung der Zertifizierungsinformation verzichtet werden, falls dem Empfänger der Nachricht die Nutzung des Directory möglich ist.

5.4.5 Sperrlisten Management

Anwendungen für einen rechtsverbindlichen Geschäftsverkehr mit Einsatz der elektronischen Signatur erfordern einen Verzeichnisdienst auch zum Abruf von Sperrlisten (alternativ können CAs auf Online-Sperrbenachrichtigungsmechanismen wie z. B. das OCSP-Protokoll zurückgreifen).

Jede CA ist verantwortlich für die Ausgabe der von ihr gesperrten Zertifikate. Für die Sperrung eines Zertifikates können mehrere Gründe ausschlaggebend sein:

- das Schlüsselpaar wurde kompromittiert oder es besteht ein begründeter Verdacht der Kompromittierung und
- organisatorische Gründe (z. B. die Entfernung des Teilnehmernamens aus dem System)
- falsche Angaben im Zertifikat.

In Anhang A.4 ist die ASN.1 Syntax einer Sperrliste wiedergegeben.

Es ist das Format „CRLv2“ nach der Spezifikation X.509v3 (ITU-X.509 97) zu unterstützen. Eine Sperrliste besteht aus den folgenden Einträgen:

- **Signatur** (Identität des Signaturalgorithmus und zugehörige Parameter)

Dieses Datenelement entspricht dem gleichnamigen Datenfeld im Zertifikat.

- **Erzeuger der Sperrliste**

Name der CA, die die Sperrliste signiert hat.

- **Ausgabedatum**

Datum der Listenerstellung.

- **nächste Aktualisierung**

Hier wird der vorgesehene Zeitpunkt zur Verteilung der nächsten aktualisierten Sperrliste angegeben.

- **Liste der gesperrten Zertifikate**

Für jedes gesperrte Zertifikat wird die zugehörige Seriennummer und der Zeitpunkt der Sperrung angegeben.

Die CRL's werden sofort nach einer Sperrung, spätestens alle 2 Wochen aktualisiert.

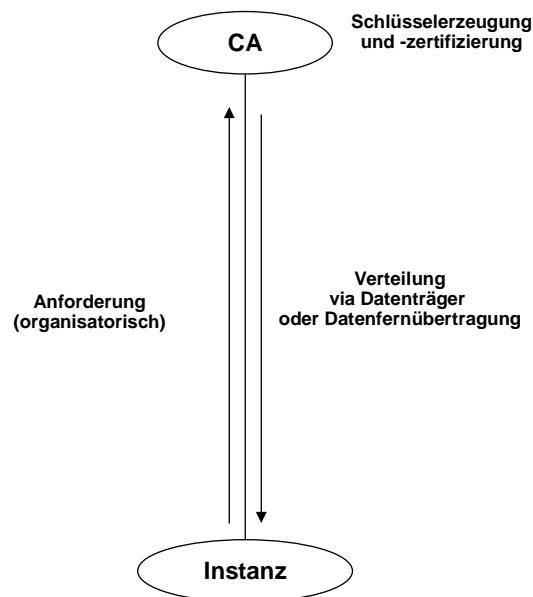
5.4.6 Schlüsselverteilung via Datenträger

Anwendungen für einen rechtsverbindlichen Geschäftsverkehr mit Einsatz der elektronischen Signatur erfordern grundsätzlich die zentrale Erstellung und Verteilung der Teilnehmerzertifikate. Die erzeugte und zertifizierte Schlüsselinformation wird von der CA an den Teilnehmer übermittelt.

Als Datenträger sollen bevorzugt Chipkarten verwendet werden. Die Absicherung von Schreib- und Leseinformationen auf der Chipkarte über eine PIN ermöglicht die Wahrung der Vertraulichkeit von sensiblen Daten (privater Schlüssel). Aus verfahrenstechnischen Gründen sind zunächst die MailTrust-Spezifikationen V2 (Cryptoki-Schnittstelle), welche auf den PKCS#11 Spezifikationen basieren, zu unterstützen.

Soweit Disketten als Datenträger im Sinne einer Übergangslösung verwendet werden, ist die Formatbeschreibung gemäß PKCS#12 (Standard zum Austausch persönlicher Informationen) „für den Transport geheimer Schlüssel und Zertifikaten“ vorzusehen.

Die folgende Übersicht veranschaulicht die spezifischen Vorgänge.



Bei einer Schlüsselverteilung an die Teilnehmer unter Verwendung eines Datenträgers (Chipkarte oder Diskette) ist der private Schlüssel des Teilnehmers (vom Typ privater RSA-Schlüssel) vom Trust Center an den Teilnehmer zuzustellen.

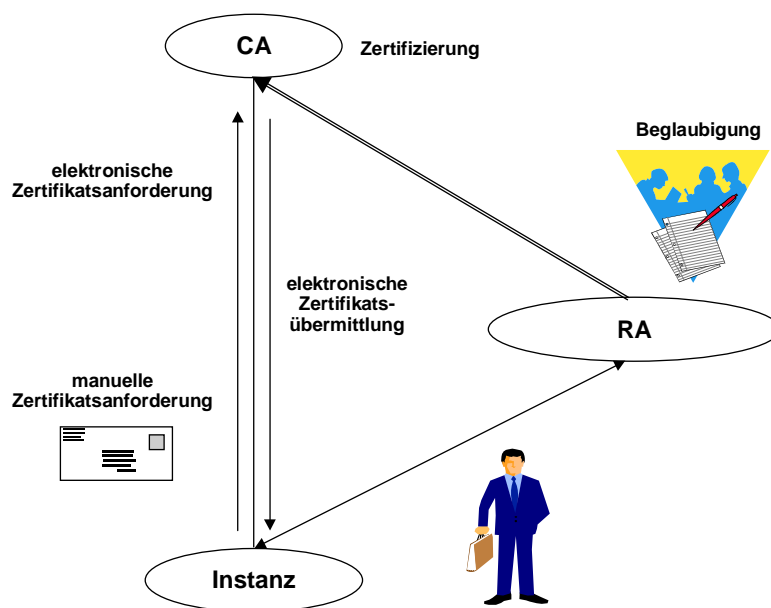
Die von der CA zur Verfügung gestellte Schlüsselinformation wird per Datenfernübertragung übermittelt oder von einem Datenträger (z.B. Chipkarte) gelesen und in die lokale Schlüsselverwaltung integriert. Dabei ist die lokale Schlüsselverwaltung abhängig von der jeweiligen Systemumgebung (Hardwareausstattung).

5.5 Registrierungsstelle (RA = Registration Authority)

Eine Identifikation und Authentikation des Teilnehmers kann durch eine Registrierungsstelle unterstützt werden, die auch räumlich getrennt von der CA agieren kann. Die Beglaubigung des Antrages wird von der RA an die CA übermittelt. In diesem Fall wird die RA a priori als vertrauenswürdige Instanz angesehen.

Die Zertifikatsübermittlung durch die CA an den Teilnehmer erfolgt in der beschriebenen elektronischer Form. Bei einer zentralen Erstellung von Zertifikaten kann die RA auch für die Ausgabe der Datenträger (z.B. Chipkarte) eingesetzt werden.

Die beschriebenen Abläufe für eine Certification Request (Zertifikatsanforderung) sind im nachfolgend veranschaulicht:



Die CA nimmt die Zertifizierung der Schlüssel vor, muss sich dabei jedoch in geeigneter Form davon überzeugen, dass der Antragsteller tatsächlich derjenige ist, der er zu sein vorgibt. Dies bedeutet, dass jeder Antragsteller einer Zertifizierung in Person mit entsprechenden beweiskräftigen Unterlagen beim Trust Center bzw. RA vorstellig werden muss.

Zur Beglaubigung des Antrages sind vom Antragsteller neben dem ausgefüllten Antrag auf Zertifizierung die nachstehend genannten Unterlagen vorzulegen:

- der Ausdruck seines öffentlichen Schlüssels
- Personalausweis, Reisepass oder Führerschein (Original und 1 Kopie).

Anmerkung: Der Antrag auf Zertifizierung kann den Ausdruck des öffentlichen Schlüssels enthalten; die Dokumente müssen nicht zwingend separiert werden.

Zur Identifizierung ist nachfolgender Ablauf vorgesehen:

1. Die Identifizierung erfolgt durch Prüfung des gültigen Personalausweises (alternativ Reisepass oder Führerschein) und Vergleich mit dem anwesenden Antragsteller. Handelt es sich um einen Unternehmensbeauftragten, so ist ergänzend der Beschäftigungsnachweis vorzulegen.
2. Nach eindeutiger Identifizierung unterschreibt der Antragsteller sowohl seinen Antrag als auch den Ausdruck seines öffentlichen Schlüssels.

Optional – nur nach gesonderter Anforderung

3. Der Mitarbeiter der CA/RA bestätigt durch seine Unterschrift auf dem Antrag sowie dem Ausdruck des öffentlichen Schlüssels, dass er sich von der Identität des Antragstellers überzeugt hat und dass die Unterschriften auf dem Antrag und dem Ausdruck des öffentlichen Schlüssels in seiner Gegenwart geleistet wurden. Sowohl das Datum als auch der Name des identifizierenden Mitarbeiters der CA/RA müssen eindeutig erkennbar sein. Der Name ist in Druckbuchstaben zu wiederholen.

Bei der Ausgabe qualifizierter Zertifikate, die zur elektronischen Signatur eingesetzt werden, sind die besonderen Verfahren zur Authentifizierung zu beachten und die Identifizierungsverfahren entsprechend anzupassen.

5.6 Teilnehmer

Die Teilnehmer nehmen unter Verwendung technischer Hilfsmittel (Hard- und Software) als Initiatoren (Sender) bzw. eigentliche Endabnehmer (Empfänger) am System teil. Dabei kann der im Auftrag eines Teilnehmers agierende Prozess als Teilnehmer-Repräsentant angesehen werden. Diese Sichtweise wird durch den separaten Begriff "User Agent" (UA) unterstützt. Teilnehmer bzw. UA müssen nachfolgende Funktionalitäten zur Verfügung stellen:

5.7 Erzeugung und Schutz der Teilnehmerschlüssel

Grundsätzlich sollte der Client in der Lage sein, Schlüsselpaare für den Teilnehmer zu erzeugen.

An die Erzeugung und Speicherung der Teilnehmerschlüssel sind hohe Sicherheitsanforderungen zu stellen. Insbesondere muss die Vertraulichkeit des privaten Schlüssels gewährleistet sein.

Der private Schlüssel ist in einer PSE (Personal Security Environment) sicher zu speichern.

5.8 Certification Request

Eine Zertifizierungsanforderung/Zertifizierungsanfrage (ein in MIME eingebettetes PKCS#10 – Objekt) kann von einem Teilnehmer, einer RA oder einer CA erstellt werden.

Die Certification Request (Zertifikatsanforderung) besteht aus einer elektronischen Anforderung in Form eines Certification Requests, den der Teilnehmer durch seine Komponenten, sein Token oder von einer RA erstellen lassen kann und der an die CA gesendet wird. Durch die Anforderung/Anfrage wird das Zertifikat spezifiziert, welches von der CA generiert werden soll.

Für den Zertifizierungsprozess werden zwei PKI-Nachrichtentypen ausgetauscht. Die erste davon stellt die erwähnte Zertifizierungs-Anfrage dar, mit der das zu erstellende Zertifikat spezifiziert wird (self-signed) . Die zweite Nachricht (Antwort auf die Anfrage/Anforderung) enthält u.a. das erstellte Zertifikat bzw. eine Fehlermeldung.

Um die zur Zertifikatsbildung notwendigen Informationen auch über die Schlüsselinformation zu sichern, sind die Anforderungen mit den folgenden Daten zu belegen:

Ein Certification Request besteht aus drei Teilen:

- CertificationRequestInfo,
- Ein Identifier für den Signatur-Algorithmus,
- Eine elektronische Signatur des Antragstellers auf der CertificationRequestInfo.

Ein CertificationRequestInfo wiederum besteht aus:

- Der Versionsnummer der verwendeten PKCS-Version,
- Dem Distinguished Name des Antragstellers,
- Dem öffentlichen Schlüssel des Antragstellers (inklusive PK-Algorithmus),
- Eine Menge von Attributen.

Attribute werden verwendet:

- Zur Angabe von zusätzlichen Informationen über den Antragsteller, die die Certification Authority (CA) benötigt, um die Zertifizierungsanfrage bearbeiten zu können (z.B. die Adresse, an die das Zertifikat zugestellt werden soll).
- Um Attribute zu spezifizieren, die in dem zu erstellenden X.509 Zertifikat erhalten sein sollen.

Eine Zertifikatserstellung und Verteilung durch die CA für den anfordernden Teilnehmer erfolgt nur unter den Bedingungen:

- Erfolgreiche Validierung des Certification Request,
- erfolgreiche Verifizierung der Signatur bzw. des Hashwertes des öffentlichen Schlüssels.

Der Ablauf ergibt sich aus der Anwendung von X.509 und PKCS#10.

5.9 Verarbeitung von Sperrlisten

Jeder Teilnehmer bzw. UA muss die Verarbeitung von Sperrlisten (Certificate Revocation List, CRL) unterstützen. Dazu sind die folgenden Funktionalitäten bereitzustellen:

- Anforderung zur Sperrung eines Zertifikats,
- Anforderung von Sperrlisten von einer CA,
- Echtheits-Verifizierung von Sperrlisten (Sperrlisten sind von der CA signiert),
- Abgleich der Sperrliste mit lokaler Zertifikatsliste (Adreßliste),
- periodisches Überprüfen des Gültigkeitszeitraums einer Sperrliste (dadurch kann das Anfordern einer neuen Sperrliste ausgelöst werden)

6 Anhang

Um Kompatibilität zwischen den verschiedenen Teilnehmern erreichen zu können, müssen neben den kryptographischen Sicherheitsverfahren auch die Strukturen sicherheitsrelevanter Daten so weit wie nötig festgelegt werden. Diese Strukturen sind kompatibel zu den Datenstrukturen und Zertifikaten nach INTERNET-Konventionen (diverse RFC) sowie nach ITU-T (X.500-Serie) festzulegen.

6.1 ASN.1 Syntax relevanter Datenstrukturen

6.1.1 Öffentlicher und privater Schlüssel nach X.509

Öffentliche und private RSA-Schlüssel haben die folgende Syntax:

```
RSAPublicKey ::= SEQUENCE {  
    modulus      INTEGER,      /* n */  
    publicExponent INTEGER } /* e */
```

```
RSAPrivateKey ::= SEQUENCE {  
    modulus      INTEGER,      /* n */  
    secretExponent INTEGER } /* d */
```

Alternativ dazu, kann das Format des privaten Schlüssels auch wie folgt realisiert werden:

```
RSAPrivateKey ::= SEQUENCE {  
    prime1      INTEGER,      /* p */  
    prime2      INTEGER } /* q */
```

In diesem Fall kann mit den Strukturen für den öffentlichen und privaten Schlüssel bei Bedarf eine an PKCS angelehnte erzeugt werden. Der erforderliche Speicherplatz lässt sich gegenüber diesem Format minimieren. Dieser Effekt ist besonders dann von Vorteil, wenn die Implementierung auf Systemen erfolgen muss, die relativ wenig Speicherplatz zur Verfügung haben (z. B. Chipkarten). Bei Anwendung des privaten Schlüssels sind allerdings die zugehörigen Parameter - insbesondere der geheime Exponent - erst zu erzeugen.

Die Konventionen können im Rahmen der Pilotverfahrens und der Interoperabilitätstests angepasst und ergänzt werden.

6.1.2 X.509v3-Zertifikat, Zertifizierungspfad

X.509-Zertifikate sowie Zertifizierungspfade werden durch die folgenden Strukturen in ASN.1 Syntax definiert:

```
Certificate ::= SIGNED SEQUENCE {
    version [0]          Version DEFAULT v1988,
    serialNumber         CertificateSerialNumber,
    signature            AlgorithmIdentifier,
    issuer               Name,
    validity             Validity,
    subject              Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo }

IssuerUniqueIdentifier      Name, {OPTIONAL}
SubjectUniqueIdentifier     Name, {OPTIONAL}

Version ::= INTEGER { v1988(0) } (Version 1 oder 3)

CertificateSerialNumber ::= INTEGER
Validity ::= SEQUENCE {
    notBefore      GeneralizedTime,
    notAfter       GeneralizedTime }
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm      AlgorithmIdentifier,
    subjectPublicKey BIT STRING }

Certification Extensions
AlgorithmIdentifier ::= SEQUENCE {
    algorithm      OBJECT IDENTIFIER,
    parameters    ANY DEFINED BY algorithm OPTIONAL }
Certificates ::= SEQUENCE {
    certificate     Certificate,
    certificationPath ForwardCertificationPath OPTIONAL }
```

Die Konventionen können im Rahmen der Pilotverfahrens und der Interoperabilitätstests angepasst und ergänzt werden.

6.1.3 Sperrliste

Die folgende ASN.1 Syntax definiert das Format einer Sperrliste [:

```
CertificateRevocationList ::= SIGNED SEQUENCE {  
    signature           AlgorithmIdentifier,  
    issuer              Name,  
    lastUpdate         GeneralizedTime,  
    nextUpdate        GeneralizedTime,  
    revokedCertificates SEQUENCE OF CRLEntry OPTIONAL }
```

```
CRLEntry ::= SEQUENCE {  
    userCertificate      SerialNumber,  
    revocationDate      GeneralizedTime }
```

Die Konventionen können im Rahmen der Pilotverfahrens und der Interoperabilitätstests angepasst und ergänzt werden.

6.2 ASN.1 Syntax relevanter Makros

6.2.1 Signierte Struktur

Die folgende ASN.1 Syntax eines Makros definiert das Format einer signierten Struktur:

```
SIGNED MACRO ::=
BEGIN

TYPE NOTATION ::= type (ToBeSigned)

VALUE NOTATION ::= value (VALUE

    SEQUENCE {
        ToBeSigned,
        AlgorithmIdentifier (des Signaturverfahrens),
        ENCRYPTED OCTET STRING (OCTET STRING ist der Hashwert
        vom Datenelement "ToBeSigned") }
    )
END of SIGNED
```

Die Konventionen können im Rahmen der Pilotverfahrens und der Interoperabilitätstests angepasst und ergänzt werden.

6.2.2 ASN.1 Syntax einer Signatur

Die folgende ASN.1 Syntax definiert das Format einer Signatur ;

```
SIGNATURE MACRO ::=
BEGIN

TYPE NOTATION ::= type (ofSignature)

VALUE NOTATION ::= value (VALUE

    SEQUENCE {
        AlgorithmIdentifier (des Signaturverfahrens),
        ENCRYPTED OCTET STRING (OCTET STRING ist der Hashwert
        vom Datenelement "ofSignature") }
    )

END of SIGNATURE
```

Die Konventionen können im Rahmen der Pilotverfahrens und der Interoperabilitätstests angepasst und ergänzt werden.

6.3 Kommunikationssystem

6.3.1 Grundsatz

Die für das Routing der Daten erforderlichen Informationen sind zu liefern. Im Rahmen des Datenaustausches werden zwischen zwei Kommunikationspartnern Nutzdateien ausgetauscht. Dabei können, in Abhängigkeit der vorhandenen Übertragungswege eine oder mehrere Stellen als Vermittlungsstellen fungieren. Unabhängig von der Art der Daten sollen die kommunizierenden Stellen die notwendigen Informationen erhalten, die es erlauben, Nutzdaten ohne Kenntnis der eigentlichen Dateninhalte zu befördern.

6.3.2 Voraussetzungen und Forderungen für den Datenaustausch auf Basis von S/MIME (E-Mail Kommunikation)

Aufbauend auf diesen Anforderungen sind bestimmte Informationen in den Kopf-Feldern der E-Mail-Nachrichten (RFC 822) zu liefern. Das Felder SUBJECT ist für die Weitergabe der Informationen zu verwenden. Der Feld-Inhalt und Bedeutung ergibt sich aus den Routing-Informationen des bisherigen Auftragsatzes.

SUBJECT:

- Verfahrenskennung (5 Stellen)
- Transfer_Nummer (3 Stellen)
- Verfahrens_Kennung_Spezifikation (5 Stellen)

- IK Absender, Ersteller der Daten (15 Stellen)
- IK physikalischer Absender (15 Stellen)
- IK Empfänger, Datennutzer (15 Stellen)
- IK physikalischer Empfänger (15 Stellen)

- Dateiname (11 Stellen)
- Datum der Erstellung der Nutzdaten (14 Stellen)
- Dateigröße Nutzdaten in Bytes verschlüsselt oder komprimiert (12 Stellen)
- Dateigröße Nutzdaten in Bytes komprimiert und verschlüsselt (12 Stellen)

Die weiteren notwendigen Informationen zu den Nutzdaten ergeben sich aus den MIME-Spezifikationen zum RFC-822-Header.

Die Konventionen können im Rahmen der Pilotverfahrens und der Interoperabilitätstests angepasst und ergänzt werden.

6.3.3 Voraussetzungen und Forderungen für den Datenaustausch signierter und verschlüsselter Datenobjekte (Datenträger und sonstige Datenfernübertragungsverfahren)

Das S/MIME-basierende Verfahren regelt zunächst den bilateralen, signierten und verschlüsselten Datenaustausch mittels E-Mail. Dieses Verfahren berücksichtigt nicht die Zustellung von Datenträger mit signierten und verschlüsselten Datenobjekte sowie andere Datenfernübertragungsverfahren, wie z.B. ftp, http, FTAM etc. sowie die Nutzung von Weiterleitungsstellen ohne Entschlüsselungsbefugnis.

Zur Nutzung von anderen Übertragungsprotokollen (HTTP, FTAM usw.) sowie alternativen Datenfernübertragungsverfahren z. B. auf Datenträger werden Datenobjekte entsprechend der PKCS#7 – Syntax signiert und verschlüsselt.

S/MIME ist nicht auf E-Mail beschränkt und kann von anderen S/MIME konformen Transportmechanismen genutzt werden z. B. HTTP. Daher werden im Zusammenhang mit der Konzeption der Umstellungs-/Migrations-Phase 2 entsprechende Festlegungen getroffen.

Die Organisationen der Beteiligten im Datenaustausch sieht vor, dass Datenpakete auch über Dritte (sog. Weiterleitungsstellen) vermittelt werden, die nicht befugt sind, die Nutzdaten zu entschlüsseln. Dementsprechend müssen die Transportinformationen begleitend zu den Nutzdaten unverschlüsselt übermittelt werden.

Die signierten und verschlüsselten Nutzdaten werden von einer Auftragsatzdatei (siehe 3.2 der Richtlinien für den Datenaustausch mit den gesetzlichen Krankenkassen) begleitet, die alle relevanten Transportinformationen in unverschlüsselter Form enthält.

Die Rahmenbedingungen werden in der jeweils geltenden Fassung der Technischen Richtlinien für den Datenaustausch mit den gesetzlichen Krankenkassen beschrieben (zur Zeit Version 4.9.7 gültig ab 01.11.2008).

Literaturverweise:

- [1] RFC 822 Standard for the Format of Internet Text Messages
- [2] RFC 1778 LDAP v2 Light-weight Directory Access Protocol
- [3] RFC 2311 S/MIME Version 2 – Message Specification
- [4] RFC 2312 S/MIME Version 2 – Certificate Handling
- [5] RFC 2632 S/MIME Version 3 – Certificate Handling
- [6] RFC 2633 S/MIME Version 3 – Message Specification
- [7] PKCS#7
RSA Laboratories. PKCS#7: Cryptographic Message Syntax Standard, Version 1.5, November 1993
- [8] PKCS#1
RSA Laboratories. PKCS#1: RSA Encryption Standard. Version 1.5, November 1993
- [9] PKCS#10
RSA Laboratories. PKCS#10: Certification Request Syntax Standard. Version 1.0, November 1993[8] RFC1321
R. Rivest. RFC 1321; The MD5 Message Digest Algorithm
- [10] PKCS#11
RSA Laboratories. PKCS#11: Cryptographic Token Interface Standard Version 2.01, 22.12.1997
- [11] ASN.1
X.208 CCITT Recommendation X.209: Specification of Abstract syntax Notation One (ASN.1), 1988
X.209 CCITT Recommendation X.209: Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1), 1988
- [12] X.509
CCITT. Recommendation X.509: The Directory-Authentication Framework. 1988.
- [13] X.500
CCITT. Recommendation X.500: The Directory Overview and Concepts, models and Services. 1988.
- [14] MTRUST
TeleTrust: MailTrust Spezifikationen Version 2
- [15] ISIS-MTT
Einheitlicher Interoperabilitäts-Standard der Trustcenter ISIS (Industrial Signature Interoperability Specification)
- [16] OCSP
Online Certificate Status Protocol